IN THE CLAIMS

PLEASE AMEND THE CLAIMS AS FOLLOWS:

1. (currently amended) A method of classifying a message transmitted over a network, comprising:

maintaining a reputation table in memory, the reputation table including information regarding a plurality of address-domain pairs, each address-domain pair indicating an IP address and an associated domain of a previously received message, the information regarding each address-domain pair including one or more classification variables, the one or more classification variables decaying with time;

executing instructions stored in a computer readable storage medium to:

determine the domain from which the message is purported to be sent[[;]],

identify that the determined domain appears on a whitelist,

~~executing instructions stored in a computer readable storage medium to~~ determine an IP address ~~from the message, the IP address~~ corresponding to a device from which the message was relayed, ~~at some point in transmission of the message;~~

~~executing instructions stored in a computer readable storage medium to~~ associate the domain with the IP address to create an ~~IP address and~~ address-domain pair;

~~executing instructions stored in a computer readable storage medium to~~ classify the message ~~according to the IP address and domain pair based on one or more classification variables associated with the IP address and domain pair; and executing instructions stored in a computer readable storage medium to assign~~ based on a score assigned to the ~~IP address and~~ address-domain pair, the score comprising a ratio of a first classification variable of the address-domain pair to a second classification variable of the address-domain pair as indicated by the reputation table, and ~~the one or more classification variables decaying with time~~

override the whitelist based on the score assigned to the address-domain pair, wherein the message is classified as spam even though the domain of the message appears on the whitelist.

2. (cancelled).

3. (currently amended) The method of claim 1, wherein classifying the message ~~includes comparing the IP address and domain pair with a related IP address and~~ is further based on classification variables associated with another address-domain pair, the other address-domain pair having a related IP address or related domain.

4. (currently amended) The method of claim 1, wherein classifying the message ~~includes checking~~ is further based on classifications of other messages associated with the domain of the message, the other messages further being associated with ~~and different~~ IP addresses other than the IP address of the message.

5. (original) The method of claim 1, wherein a plurality of IP addresses is associated with the domain.

6. (original) The method of claim 1, wherein the IP address is associated with a plurality of domains.

7. (original) The method of claim 1, wherein the IP address is a boundary IP address.

8. (original) The method of claim 1, wherein the IP address is preconfigured.

9. (original) The method of claim 1, wherein the IP address is preconfigured to be one hop from a gateway IP address.

10. (original) The method of claim 1, wherein the IP address is learned.

11. (original) The method of claim 1, wherein the IP address is adaptively determined.

12. (cancelled).

13. (currently amended) The method of claim [[1]] 10, wherein the IP address is a boundary IP address and wherein the boundary IP address is learned by detecting a pattern in a certain number of previously received messages.

14. (previously presented) The method of claim 1, wherein determining the domain from which the message is purported to be sent includes identifying the stated sender domain associated with the message.

15. (previously presented) The method of claim 1, wherein the domain is a domain associated with a boundary IP address.

16. (currently amended) The method of claim 1, wherein classifying the message is further based on ~~includes~~ consulting a white list.

17. (currently amended) The method of claim 1, wherein classifying the message is further based on ~~includes classifying the message~~ based on previous classifications made to the ~~IP address and~~ address-domain pair.

18. (cancelled)

19. (previously presented) The method of claim 1, wherein assigning the score includes determining a spam ratio.

20. (previously presented) The method of claim 1, wherein assigning the score includes determining a spam rate.

21. (previously presented) The method of claim 1, wherein assigning the score includes determining an estimated instantaneous spam rate.

22. (cancelled)

23. (currently amended) The method of claim 1, wherein classifying the message includes giving a classification variable greater weight relative to another classification variable.

24. (currently amended) The method of claim 1, wherein classifying the message includes giving a classification variable associated with user classification greater weight relative to a classification variable associated with computer classification.

25. (currently amended) The method of claim 1, wherein classifying the message includes giving an indeterminate classification a fraction of the weight of a good classification.

26. (currently amended) The method of claim 1, wherein ~~classifying includes consulting a~~ the reputation table is indexed by IP address and domain.

27. (currently amended) The method of claim 1, wherein ~~classifying includes consulting a table indexed by IP address and domain wherein~~ each cell of the reputation table includes information about previous classifications.

28. (currently amended) The method of claim 1, further comprising providing [[a]] the classification of the message based on the ~~IP address and~~ address-domain pair as input to another classifier.

29. (currently amended) The method of claim [[1]] 28, ~~further including providing a classification based on the IP address and domain pair as input to~~ wherein the other classifier is a Bayesian classifier.

30. (currently amended) The method of claim 1, wherein classifying the message is further ~~includes classifying the message~~ based on a score assigned to the IP address.

31. (currently amended) The method of claim 1, wherein classifying the message is further ~~includes classifying the message~~ based on a score assigned to the domain.

32. (currently amended) The method of claim 1, ~~wherein classifying includes classifying the message based on the domain and~~ further comprising determining that the message was forged based on the score assigned to the domain.

33. (currently amended) The method of claim [[1]] 30, ~~wherein classifying includes~~ further comprising determining [[a]] the score [[for]] assigned to the IP address.

34. (currently amended) The method of claim [[1]] 31, ~~wherein classifying includes~~ further comprising determining [[a]] the score [[for]] assigned to the domain.

35. (currently amended) A computer-readable storage medium having embodied thereon a program, the program being executable by a processor to perform a method for classifying a message, the method comprising:

maintaining a reputation table including information regarding a plurality of address-domain pairs, each address-domain pair indicating an IP address and an associated domain of a previously received message, the information regarding each address-domain pair including one or more classification variables, the one or more classification variables decaying with time;

determining [[a]] the domain from which the message is purported to be sent;

identifying that the determined domain appears on a whitelist,

determining an IP address from which the message was relayed ~~at some point in transmission of the message~~;

associating the domain with the IP address to create an ~~IP address and~~ address-domain pair;

classifying the message ~~according to the IP address and domain pair based on one or more classification variables associated with the IP address and domain pair; and assigning~~ based on a score assigned to the ~~IP address and~~ address-domain pair, the score comprising a ratio of a first classification variable of the address-domain pair to a second classification variable of the address-domain pair as indicated by the reputation table, and ~~the one or more classification variables decayed with time~~

overriding the whitelist based on the score assigned to the address-domain pair, wherein the message is classified as spam even though the domain of the message appears on the whitelist.

.

36. (cancelled)